PATENT APPLICATION TRANSMITTAL LETTER (Large Entity)	Docket No. 112857-221

#5

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Tomoyuki Nakano et al.

For: **AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AUTHENTICATION APPARATUS AND AUTHENTICATION METHOD THEREFOR**

Enclosed are:

- ☒ Certificate of Mailing with Express Mail Mailing Label No. **EL416274860US**
- ☒ **thirteen** sheets of drawings.
- ☒ A certified copy of a **Japan** application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☒ Other: **Postcard**

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	20	- 20 =	0	x	$18.00	$0.00
Indep. Claims	4	- 3 =	1	x	$80.00	$80.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$710.00
					TOTAL FILING FEE	$790.00

- ☒ A check in the amount of **$790.00** to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **02-1818** as described below. A duplicate copy of this sheet is enclosed.
  - ☐ Charge the amount of as filing fee.
  - ☒ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: **April 30, 2001**

Signature

William E. Vaughan (Reg. No. 39,056)
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690

cc:

SONY P06490US00 #5

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ４月２８日

出 願 番 号
Application Number: 特願２０００－１３１８７２

出 願 人
Applicant (s): ソニー株式会社

２００１年 ３月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０１７７５１

【書類名】　特許願
【整理番号】　0000439304
【提出日】　平成12年 4月28日
【あて先】　特許庁長官　近藤　隆彦　殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内
　【氏名】　中野　智行
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内
　【氏名】　板橋　達夫
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100082740
　【弁理士】
　【氏名又は名称】　田辺　恵基
【手数料の表示】
　【予納台帳番号】　048253
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9709125
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証システム、認証方法、認証装置及びその方法

【特許請求の範囲】

【請求項１】

利用者に固有の共通鍵暗号方式による共通鍵を保持する情報保持媒体と、

各上記利用者ごとの上記共通鍵暗号方式による共通鍵と、公開鍵暗号方式による秘密鍵及び公開鍵とを保持する認証装置と、

上記認証装置と通信自在に接続され、公開鍵暗号方式による上記利用者の認証を行うための機能が実装された情報処理装置と

を具え、

上記認証装置は、

上記情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の上記情報保持媒体に保持された上記共通鍵と、自己が保持する当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う

ことを特徴とする認証システム。

【請求項２】

上記情報保持媒体は、可搬型である

ことを特徴とする請求項１に記載の認証システム。

【請求項３】

利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させる第１のステップと、

情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の上記情報保持媒体に保持された上記共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行う第２のステップと、

上記利用者を認証できた場合にのみ、上記情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う第３のステップと

を具えることを特徴する認証方法。

【請求項４】

上記情報保持媒体は、可搬型である

ことを特徴とする請求項３に記載の認証方法。

【請求項５】

各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する保持手段と、

外部の情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の上記共通暗号方式による上記共通鍵と、上記保持手段に保持された当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、上記保持手段に保持された当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う処理手段と

を具えることを特徴とする認証装置。

【請求項６】

各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する第１のステップと、

外部の情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の上記共通暗号方式による上記共通鍵と、上記保持手段に保持された当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、上記保持手段に保持された当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う第２のステップと

を具えることを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は認証システム、認証方法、認証装置及びその方法に関し、異なる種類の暗号方式の利点を効率良く利用し暗号処理し得る認証装置に適用して好適なものである。

【０００２】

【従来の技術】

従来、この種の認証システムの認証及び署名方式として共通鍵暗号方式と公開鍵暗号方式がある。

【０００３】

共通鍵暗号方式は、共通鍵と呼ばれる１つの暗号鍵を用い、共通鍵で暗号化した情報を同一の共通鍵で復号化する暗号方式である。共通鍵暗号方式は、暗号処理及び復号処理を短時間で行うことができるため、例えばＩＣカードに格納された電子マネーや定期券情報という高速処理が要求される情報を処理する場合に利用される。

【０００４】

また公開鍵暗号方式は、公開鍵及び暗号鍵と呼ばれる２つの暗号鍵を用いて、一方の暗号鍵で情報を暗号化したり、暗号化された情報を他方の暗号鍵で復号化する暗号方式である。公開鍵暗号方式は、かかる共通鍵暗号方式と比較して処理速度が遅いものの情報の漏洩に対する安全性が高く、インターネット等のネットワーク上で決済を行うときなどの匿名性が必要な場合に利用される。

【０００５】

そして公開鍵暗号方式を用いる場合、ＩＣカードには当該ＩＣカードを使用する本人を証明する証明書と暗号鍵とが格納され、暗号処理を行うためのモジュールとして利用される。

【０００６】

【発明が解決しようとする課題】

ところで認証システムにおいては、適用分野に応じてこれら共通鍵暗号方式及び公開鍵暗号方式を使い分けている。

【０００７】

しかしながら近年では、一枚のＩＣカードで効率良く認証や決済を行い得るよ

うにするために、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせ持つ暗号方式の統合が望まれている。

【０００８】

また認証システムにおいては、ＩＣカードに格納された証明書の正当性を検証する手段はあるが、当該ＩＣカードが実際、正当に使用されているか否かを検証する手段がないという問題があった。

【０００９】

さらに認証システムにおいては、ＩＣカードが紛失された場合、ネットワーク上に設けられた認証局から定期的に配付される証明書の失効リストに基づいてＩＣカードに対する認証や決済等の手続きを停止するため、ネットワーク上のすべてのポイントで即時かかるＩＣカードの使用が停止されないという問題があった。

【００１０】

本発明は以上の点を考慮してなされたもので、認証に対する安全性及び高速性を向上させ得る認証システム、認証方法、認証装置及びその方法を提案しようとするものである。

【００１１】

【課題を解決するための手段】

かかる課題を解決するために本発明においては、認証システムにおいて、利用者に固有の共通鍵暗号方式による共通鍵を保持する情報保持媒体と、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による秘密鍵及び公開鍵とを保持する認証装置と、認証装置と通信自在に接続され、公開鍵暗号方式による利用者の認証を行うための機能が実装された情報処理装置とを設け、認証装置が、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵と、自己が保持する当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにした。この結果この認証システムによれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせ

もたせた利用者認証を行うことができる。

【００１２】

また本発明においては、認証方法において、利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させる第１のステップと、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行う第２のステップと、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う第３のステップとを設けるようにした。この結果この認証方法によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【００１３】

さらに本発明においては、認証装置において、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する保持手段と、外部の情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の共通暗号方式による共通鍵と、保持手段に保持された当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、保持手段に保持された当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う処理手段とを設けるようにした。この結果この認証装置によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【００１４】

さらに本発明においては、認証方法において、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する第１のステップと、外部の情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の共通暗号方式による共通鍵と、保持手段に保持された当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、保持手段に保持された当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式

で行わせるための所定の処理を行う第２のステップとを設けるようにした。この結果この認証装置によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【００１５】

【発明の実施の形態】

以下図面について、本発明の一実施形態に形態を詳述する。

【００１６】

（１）本実施の形態によるネットワークシステムの構成

図１において、１は全体として本実施の形態によるネットワークシステムを示し、サービスプロバイダ２に設置されたＷＷＷ(World Wide Web)サーバ３と、利用者端末４と、認証センタ５に設置されたセキュリティサーバ６とがインターネット７を介して接続されることにより構成されている。

【００１７】

利用者端末４は、図２に示すように、ＣＰＵ (Central Processing Unit)１０と、後述のような各種処理を実行するためのプログラムが格納されたＲＯＭ(Read Only Memory)１１と、ＣＰＵ１０のワークメモリとしてのＲＡＭ(Randam Access Memory)１２と、入出力インターフェイスとしての入出力部１４とがバス１３を介して接続され、また当該入出力部１４にモデム等からなるネットワークインターフェイス１５と、ＩＣカード読書き装置９と、キーボード、モニタ及びマウス等からなるコンソール１７と、ハードディスク装置等からなる記憶装置１８とが接続されて構成された一般的なパーソナルコンピュータである。

【００１８】

また記憶装置１８には、ＷＷＷブラウザプログラム１９と、共通鍵暗号方式や公開鍵暗号方式に応じた暗号処理を管理するプログラムからなる暗号処理ライブラリ２５と、かかるＩＣカード読書き装置９用のＩＣカードドライバ２１とが記憶されている。

【００１９】

そしてＣＰＵ１０は、記憶装置１８に記憶されたＷＷＷブラウザプログラム１９をＲＡＭ１２上で展開して実行することにより、ＷＷＷブラウザ２２（図１）

として機能し、ネットワークインターフェイス１５を介してインターネット７上で情報の送受信を行い得るようになされている。

【００２０】

またＣＰＵ１０は、記憶装置１８に記憶された暗号処理ライブラリ２０のプログラムをＲＡＭ１２上で展開して実行することにより、暗号処理モジュール２３（図１）として機能し、暗号処理を管理する。

【００２１】

またWWWブラウザ２２と暗号処理モジュール２３との間には、例えばＲＳＡ社が提供するＰＫＣＳ#11(Public Key Cryptography Standerd #11)２４規格のＡＰＩ(Application Program Interface) が設けられており、WWWブラウザ２２と暗号処理モジュール２３との間で情報の交換を容易にしている。

【００２２】

さらにＣＰＵ１０は、記憶装置１８に記憶されたＩＣカードドライバ２１をＲＡＭ１２上で展開して実行することにより、ＩＣカード読書き装置９を操作することができる。

【００２３】

このＩＣカード読書き装置９は、例えばブルートゥース(Bluetooth) 規格の無線機能を有しており、ＩＣカード８から無線を介して読み出した情報を記憶装置２３に送出すると共に、記憶装置２３から送出された情報を無線を介してＩＣカード８に書き込み得るようになされている。

【００２４】

実際上ＩＣカード８は、図３に示すように、バス２６にＣＰＵ２７と、ＲＯＭ２８と、ＲＡＭ２９と、かかるＩＣカード読書き装置９と無線通信し得る無線通信インターフェイス３０と、当該ＩＣカード８に割り当てられた利用者ＩＤ等の各種情報を格納したＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)３１とが接続され構成されている。

【００２５】

ＥＥＰＲＯＭ３１には、利用者ＩＤ用エリア３２と、電子有価情報用エリア３３と、共通鍵用エリア３４とが設けられており、各エリアに利用者ＩＤと、電子

有価情報と、利用者ＩＤ用エリア３６及び電子有価情報用エリア３７に対して外部からのアクセスを許可するための共通鍵とがそれぞれ書き込まれる。

【００２６】

そしてＣＰＵ２７は、ＲＯＭ２８に格納された暗号処理用プログラムをＲＡＭ２９上で展開して実行することにより、無線インタース３０を介して得た共通鍵によって暗号化された情報（以下、これを共通鍵暗号化情報と呼ぶ）を、ＥＥＰＲＯＭ３１から読み出した共通鍵で復号化する。

【００２７】

またＣＰＵ２７は、共通鍵暗号化情報がＥＥＰＲＯＭ３１から読み出した共通鍵で復号が正しく行われると、当該ＥＥＰＲＯＭ３１の各エリアへのアクセスを許可し、例えばＥＥＰＲＯＭ３１の電子有価情報用エリア３３に無線インターフェイス３０を介して得た電子有価情報を書き込むようになされている。

【００２８】

一方サービスプロバイダ２に設けられたWWWサーバ３は、図４に示すように、ＣＰＵ３６と、ＲＯＭ３７と、ＲＡＭ３８とがバス３９を介して入出力部４０に接続されていると共に、当該入出力部４０にインターネット７と接続するためのルータ等からなるネットワークインターフェイス４１と、キーボード、モニタ及びマウス等からなる管理用コンソール４２と、記憶装置４３とが接続されて構成されている。また記憶装置４３には、WWWサーバプログラム４４と、電子有価情報等のサービス用コンテンツ４５とが格納されている。

【００２９】

そしてＣＰＵ３６は、記憶装置４３に格納されたWWWサーバプログラム４４をＲＡＭ３８上で展開して実行することにより、WWWサーバ３（図１）として動作し、サービス用コンテンツ４５をネットワークインターフェイス４１を介して提供し得るようになされている。

【００３０】

これに対して認証センタ５に設けられたセキュリティサーバ６は、図５に示すように、ＣＰＵ４６と、ＲＯＭ４７と、ＲＡＭ４８とがバス４９を介して入出力部５０に接続されていると共に、当該入出力部５０にインターネット７と接続す

るためのルータ等からなるネットワークインターフェイス５１と、キーボード、モニタ及びマウス等からなる管理用コンソール５２と、記憶装置５３とが接続されて構成されている。また記憶装置５３には、セキュリティサーバプログラム５４、後述する利用者証明データベース５５及び共通鍵データベース５６が格納されている。

【００３１】

そしてかかるセキュリティサーバ６のＣＰＵ４６は、記憶装置５３に格納されたセキュリティサーバプログラム５４をＲＡＭ４８上で展開して実行することにより、セキュリティサーバ６として動作する。

【００３２】

（２）認証処理手順

ここでこのネットワークシステム１は、図６に示すように、利用者端末４が図７に示す自己を認証する認証処理手順ＲＴ１に従って認証を行うと共に、セキュリティサーバ６が図８に示す認証処理手順ＲＴ２に従って当該利用者端末４の認証を行うことにより、利用者端末４が電子有価情報を提供するＷＷＷサーバ３に対して自己の正当性を証明することができる。

【００３３】

この場合まず利用者端末４は、ＷＷＷブラウザ２２を操作して、ＷＷＷサーバ３に対し当該利用者端末４に電子有価情報を要求する。

【００３４】

このときＷＷＷサーバ３は、まずランダムな文字列からなる試用文字を生成した後、当該生成した試用文字と共に、要求元の正当性を確認するために利用者端末４が認証されるための認証要求コマンドＣ１を当該利用者端末４に送出する。

【００３５】

そして利用者端末４のＣＰＵ１０は、認証要求コマンドＣ１を受けとると、認証処理手順ＲＴ１を開始し（ステップＳＰ１）、受けとった当該認証要求コマンドＣ１及び試用文字を暗号処理モジュール２３に送出する（ステップＳＰ２）。

【００３６】

続けてＣＰＵ１０は、ＩＣカード読書き装置９を介してＩＣカード８から使用

者ＩＤを読み出し、当該読み出した使用者ＩＤと共に暗号処理モジュール２３で受けとった認証要求コマンドＣ１及び試用文字をセキュリティサーバ６へ送出する（ステップＳＰ３）。

【００３７】

セキュリティサーバ６のＣＰＵ４６は、認証要求コマンドＣ１を受けとると、認証処理手順ＲＴ２を開始し（ステップＳＰ２１）、受けとった使用者ＩＤに対応する共通鍵を、図９に示すような記憶装置５３内の共通鍵データベース５６から読み出し（ステップＳＰ２２）、当該読み出した共通鍵で共通暗号化情報を生成する。続けてＣＰＵ４６は、共通暗号化情報と共にＩＣカード認証要求コマンドＣ２を利用者端末４の暗号処理モジュール２３に送出する（ステップＳＰ２３）。

【００３８】

さらにＣＰＵ４６は、かかる使用者ＩＤに対応する証明書を、図１０に示すような記憶装置５３内の利用者証明データベース５５から読み出し、これを利用者端末４の暗号処理モジュール２３及びＷＷＷブラウザ２２を介してＷＷＷサーバ４へ予め送出しておく。

【００３９】

ここで証明書５８には、例えば利用者ＩＤが0001の場合、図１１に示すように、証明書シリアル番号と、当該証明書の有効期限情報と、利用者ＩＤと、かかる秘密鍵と対で生成された公開鍵と、電子メールのメールアドレスと、利用者の連絡先情報となどの情報が記載されている。加えて証明書５８には、秘密鍵及び公開鍵（以下、これらの一組の鍵を暗号鍵と呼ぶ）を生成する認証局のディジタル署名６０が施されており、当該証明書５８の正当性を保証している。

【００４０】

一方利用者端末４のＣＰＵ１０は、暗号処理モジュール１１においてＩＣカード認証要求コマンド及び共通鍵を受けとると、ＩＣカードドライバ２１を実行することによりＩＣカード読書き装置９を操作し（ステップＳＰ５）、当該ＩＣカード読書き装置９を介してＩＣカード８にＩＣカード認証要求コマンドＣ２及び共通暗号化情報を送出する。

【００４１】

またＩＣカード８は、ＩＣカード認証要求コマンドＣ２を受けとると、共通暗号化情報を内部に設けられたＥＥＰＲＯＭ３１内の共通鍵で認証（復号）し、当該認証結果を暗号処理モジュール２３を介してセキュリティサーバ６に送出する（ステップＳＰ５）。

【００４２】

セキュリティサーバ６のＣＰＵ４６は、受けとった認証結果によりＩＣカード８の認証が正常に行われたことを確認すると（ステップＳＰ１５）、ＷＷＷサーバ３から送信された認証要求に基づいて、利用者証明データベース５５（図６）から利用者ＩＤの秘密鍵を取得し（ステップＳＰ１６）、受けとった試用文字に当該秘密鍵でディジタル署名を施してディジタル署名書（ステップＳＰ１７）を生成し、これを利用端末４の暗号処理モジュール２３（ステップＳＰ１８）に送出する。

【００４３】

これとは反対にＣＰＵ４６は、受けとった認証結果によりＩＣカード８の認証が正常に行えなかったことを確認すると（ステップＳＰ１５）、再度利用者ＩＤを受けとり、当該利用者ＩＤに応じた共通鍵で新しい共通暗号化情報を生成し、これをＩＣカード８へ送出する。ＣＰＵ４６は、ＩＣカード８から再度認証結果を得るようになされている。

【００４４】

一方利用端末４のＣＰＵ１０は、暗号処理モジュール２３において、セキュリティサーバ６からディジタル署名書を受けとる（ステップＳＰ７）と、これをＰＫＣＳ＃1124を介してＷＷＷブラウザ１０へ送出する（ステップＳＰ８）。続けてＣＰＵ１０は、受けとったディジタル署名書を認証要求の応答としてＷＷＷサーバ３へ送出する（ステップＳＰ９）。

【００４５】

またＷＷＷサーバ３は、ディジタル署名書を受けとると、予め受けとっている利用者証明書に記載された公開鍵を用いてディジタル署名を復号化し、当該復号化が正常に行われた場合、正当な利用者端末４から電子有価情報の要求がされた

と判断する。

【００４６】

かくしてWWWサーバ３は、電子有価情報をかかる利用者端末４に電子有価情報を送出する準備を行い、当該電子有価情報に対して公開鍵で暗号化し、これにより得た暗号化電子有価情報を利用者端末４に送出することができる。

【００４７】

ここでネットワークシステム１においては、図１２に示すように、利用者端末４が図１３に示す書き込み処理手順ＲＴ３に従って書き込みを行うと共に、セキュリティサーバ６が図１４に示す書き込み処理手順ＲＴ４に従って暗号化電子有価情報を復号化してすることにより、利用者端末４が電子有価情報をＩＣカード８に書き込むことができる。

【００４８】

まずWWWサーバ３は、暗号化電子有価情報を利用者端末４のWWWブラウザ２２に送出する。

【００４９】

利用者端末４のＣＰＵ１０は、WWWブラウザ２２において暗号化電子有価情報を受けとると、書き込み処理手順ＲＴ３を開始し（ステップＳＰ２１）、受けとった暗号化電子有価情報及び復号要求コマンドＣ３を暗号処理モジュール２３に送出する（ステップＳＰ２２）。

【００５０】

続けてＣＰＵ１０は、暗号処理モジュール２３で受けとった暗号化電子有価情報及び復号要求コマンドＣ３に合わせて、ＩＣカード読書き装置９を介してＩＣカード８から読み出した使用者ＩＤをセキュリティサーバ６へ送出する（ステップＳＰ２３）。

【００５１】

セキュリティサーバ６のＣＰＵ４６は、復号要求コマンドＣ３を受けとると、書き込み処理手順ＲＴ４を開始し（ステップＳＰ４１）、まずＩＣカード８の認証を行う。ＣＰＵ４６は、受けとった使用者ＩＤに対応する共通鍵を共通鍵データベース５５から読み出し（ステップＳＰ４２）、当該読み出した共通鍵で共通

暗号化情報を生成する。続けてＣＰＵ４６は、共通暗号化情報及びＩＣカード認証要求コマンドＣ４を利用者端末４の暗号処理モジュール２３に送出する（ステップＳＰ４３）。

【００５２】

利用者端末４のＣＰＵ１０は、暗号処理モジュール２３においてＩＣカード認証要求コマンドＣ４及び共通暗号化情報を受けとると、ＩＣカードドライバ２１を操作（ステップＳＰ２４）することによりＩＣカード読書き装置９を介してＩＣカード８にＩＣカード認証要求コマンドＣ４及び共通暗号化情報を送出する。

【００５３】

ＩＣカード８は、ＩＣカード認証要求コマンドＣ４を受けとると、かかる共通暗号化情報を内部に設けられたＥＥＰＲＯＭ３１内の共通鍵で認証（復号）し、当該認証結果を暗号処理モジュール２３を介してセキュリティサーバ６に送出する（ステップＳＰ２５）。

【００５４】

セキュリティサーバ６のＣＰＵ４６は、暗号処理モジュール２３から送出された認証結果を受けとり（ステップＳＰ４４）、当該認証結果によりＩＣカード８の認証が正常に行われたことを確認すると（ステップＳＰ４５）、利用者証明データベース５５（図６）から利用者ＩＤの秘密鍵を取得し（ステップＳＰ４６）、この秘密鍵で暗号化電子有価情報を復号化する（ステップＳＰ４７）ことにより、電子有価情報を生成する。

【００５５】

続けてＣＰＵ４６は、生成した電子有価情報を共通鍵データベース５５から読み出した共通鍵で暗号化して、共通暗号化電子有価情報を生成する。

【００５６】

一方ＣＰＵ４６は、受けとった認証結果によりＩＣカード８の認証が正常に行えなかったことを確認すると（ステップＳＰ４５）、利用者端末４から利用者ＩＤを受けとり、当該利用者ＩＤに応じた共通鍵に対してＩＣカード８内で認証を行い、当該認証結果を受けとるようになされている。

【００５７】

利用端末４のＣＰＵ１０は、暗号処理モジュール２３において、セキュリティサーバ６から書き込み要求コマンドＣ５及び共通暗号化電子有価情報を受けとる（ステップＳＰ２７）と、当該共通暗号化電子有価情報をＩＣカード読書き装置９を介してＩＣカード８に送出する。

【００５８】

ＩＣカード８のＣＰＵ２７は、受けとった共通暗号化電子有価情報をＥＥＰＲＯＭ３１の共通鍵用エリア３４から読み出した共通鍵で復号化し、当該復号化して得た電子有価情報をＥＥＰＲＯＭ３１の電子有価情報用エリア３３に書き込む。

【００５９】

また利用端末４のＣＰＵ１０は、暗号処理モジュール２３において受けとった電子有価情報をＷＷＷブラウザ２２に送出する。かくしてＷＷＷブラウザ２２は、ＷＷＷサーバ３から復号化された電子有価情報を得ることができる。

【００６０】

（３）本実施の形態の動作及び効果

以上の構成において、このネットワークシステム１では、セキュリティサーバ６がＷＷＷサーバ３から与えられる利用者の認証要求に応じて、当該利用者が携帯するＩＣカード８に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、ＷＷＷサーバ３に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う。

【００６１】

従ってこのネットワークシステム１によれば、セキュリティサーバ６がＷＷＷサーバ３から与えられる利用者の認証要求に応じて、共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、ＷＷＷサーバ３に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うことにより、共通鍵暗号方式による高速性と公開鍵暗号方式による安全性とを合わせ持つことができる。

【００６２】

以上の構成によれば、このネットワークシステム１において、セキュリティサ

ーバ６がＷＷＷサーバ３から与えられる利用者の認証要求に応じて、共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、ＷＷＷサーバ３に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うことにより、共通鍵暗号方式による高速性と公開鍵暗号方式による安全性とを合わせ持つことができ、かくして認証に対する安全性及び高速性を向上し得るネットワークシステム１を実現することができる。

【００６３】

（４）他の実施の形態

なお上述の実施の形態においては、カード読み書き装置９とＩＣカード８とが無線を介して情報を受渡しする場合について述べたが本発明はこれに限らず、カード読み書き装置９とＩＣカード８とを物理的に接続して情報を受渡しするようにしても良い。

【００６４】

また上述の実施の形態においては、セキュリティサーバ６とＩＣカード８との間で認証を行った後、キュリティサーバ６で復号された電子有価情報をＩＣカード８に格納する際、再度セキュリティサーバ６とＩＣカード８との間で認証を行ってから当該電子有価情報をＩＣカード８に格納する場合について述べたが本発明はこれに限らず、セキュリティサーバ６とＩＣカード８との間で接続が確立されている限り、セキュリティサーバ６とＩＣカード８との間での認証を１回だけに行うようにしても良い。

【００６５】

さらに上述の実施の形態においては、利用者端末４からセキュリティサーバ６に対して共通鍵に基づく認証要求が与えられた際に、ＩＣカード８の認証を行う場合について述べたが本発明はこれに限らず、利用者端末４がインターネットと接続した際にセキュリティサーバ６と接続し、予めＩＣカード８の認証を行っておくようにしても良い。

【００６６】

さらに上述の実施の形態においては、電子マネーや定期券情報等の電子有価情報を扱う場合について述べたが本発明はこれに限らず、フリーウエア等の無償の

情報を扱うようにしても良い。

【００６７】

さらに上述の実施の形態においては、電子有価情報として電子マネーや定期券情報等を扱う場合について述べたが本発明はこれに限らず、電子有価情報として音楽情報や書籍情報等を扱うようにしても良い。

【００６８】

さらに上述の実施の形態においては、情報保持媒体としてＩＣカードを用いる場合について述べたが本発明はこれに限らず、演算機能やメモリ機能を有した媒体であれば良い。

【００６９】

さらに上述の実施の形態においては、セキュリティサーバ６が共通鍵で生成した暗号化情報をＩＣカード８において復号化して利用者を認証する場合について述べたが本発明はこれに限らず、ＩＣカード８が共通鍵で生成した暗号化情報をセキュリティサーバ６において復号化して利用者を認証するようにしても良い。

【００７０】

【発明の効果】

上述のように本発明によれば、利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させ、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにしたことにより、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができ、かくして認証に対する安全性及び高速性を向上させ得る認証システム、認証方法、認証装置及びその方法を実現できる。

【図面の簡単な説明】

【図１】

本実施の形態によるネットワークシステムの構成を示す略線図である。

【図２】

利用者端末の構成を示すブロック図である。

【図３】

ＩＣカードの構成を示すブロック図である。

【図４】

WWWサーバの構成を示すブロック図である。

【図５】

セキュリティサーバの構成を示すブロック図である。

【図６】

認証の様子の説明に供する略線図である。

【図７】

利用者端末の認証処理手順のフローチャートである。

【図８】

セキュリティサーバの認証処理手順のフローチャートである。

【図９】

共通鍵データベースの構成を示す略線図である。

【図１０】

利用者証明データベースの構成を示す略線図である。

【図１１】

証明書の構成を示す略線図である。

【図１２】

書き込みの様子の説明に供する略線図である。

【図１３】

利用者端末の書き込み処理手順のフローチャートである。

【図１４】

セキュリティサーバの書き込み処理手順のフローチャートである。

【符号の説明】

１……ネットワークシステム、３……WWWサーバ、４……利用者端末、６……セキュリティサーバ、８……ＩＣカード、11……暗号処理モジュール、１７、３１、４２、５３……ＣＰＵ、２３、４８、６０……外部記憶装置、６１……利用者データベース、６２……共通データベース。

【書類名】図面

【図１】

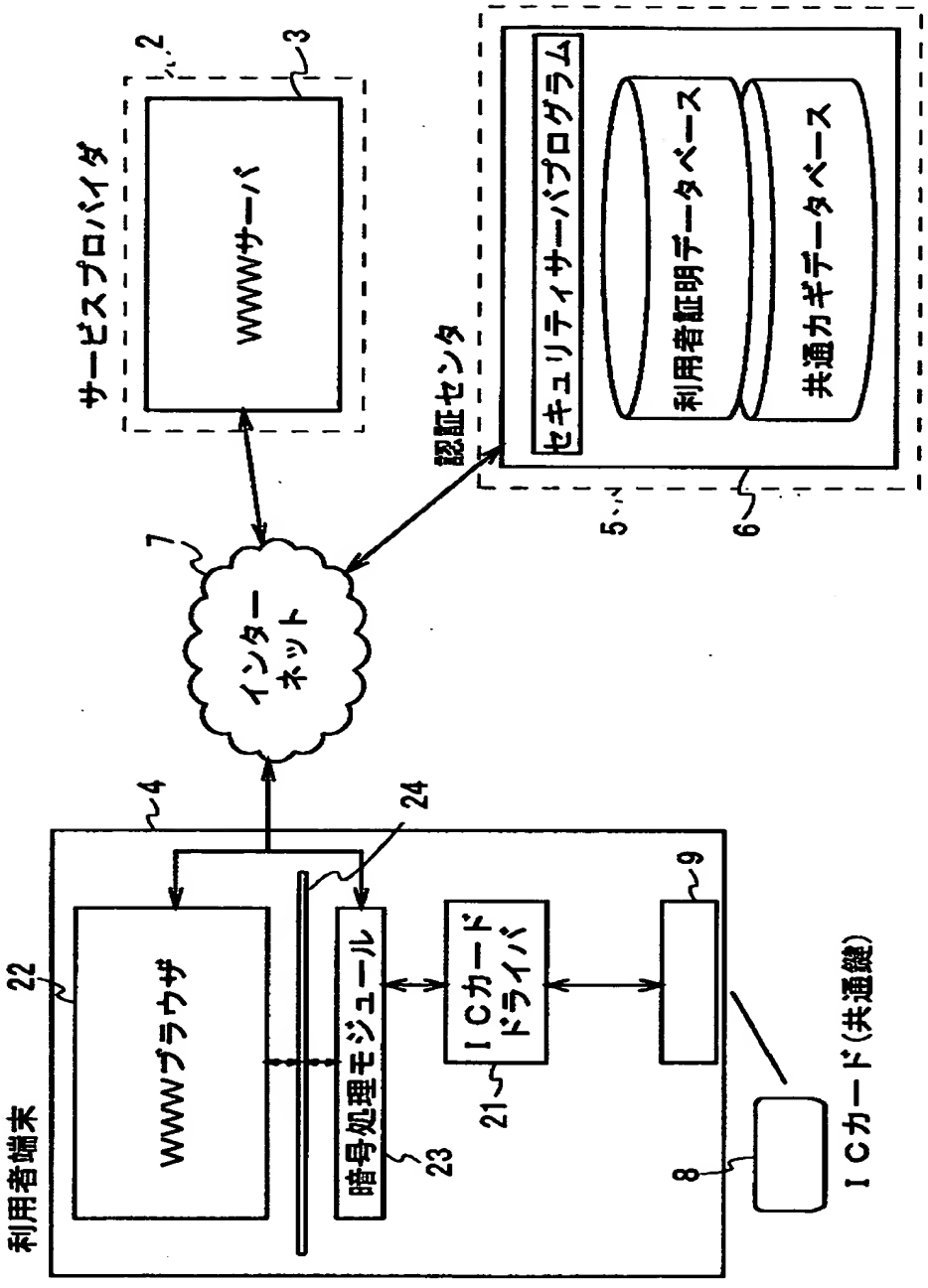

図１　ネットワークシステムの構成

【図２】

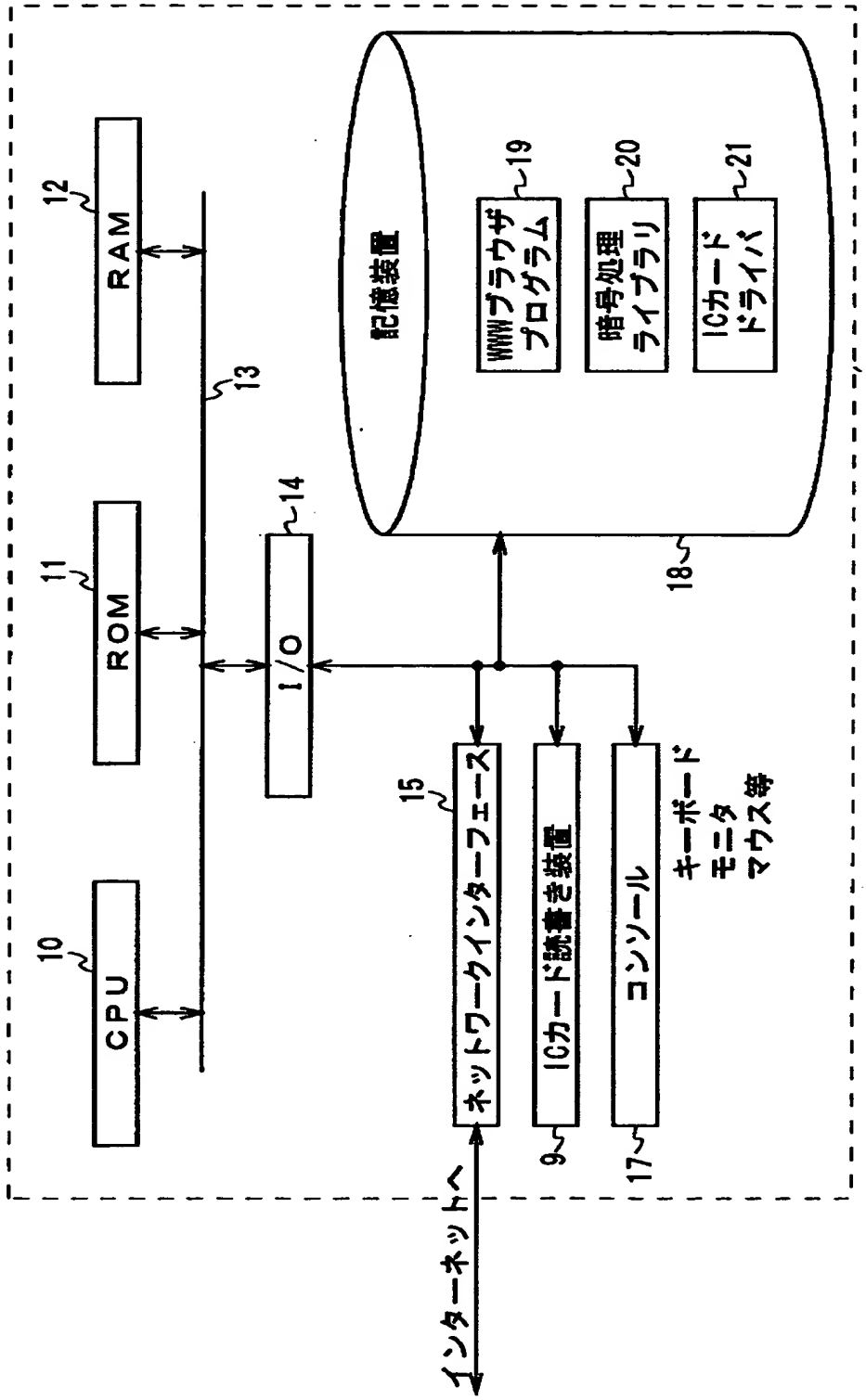

図２　利用者端末の構成

【図３】

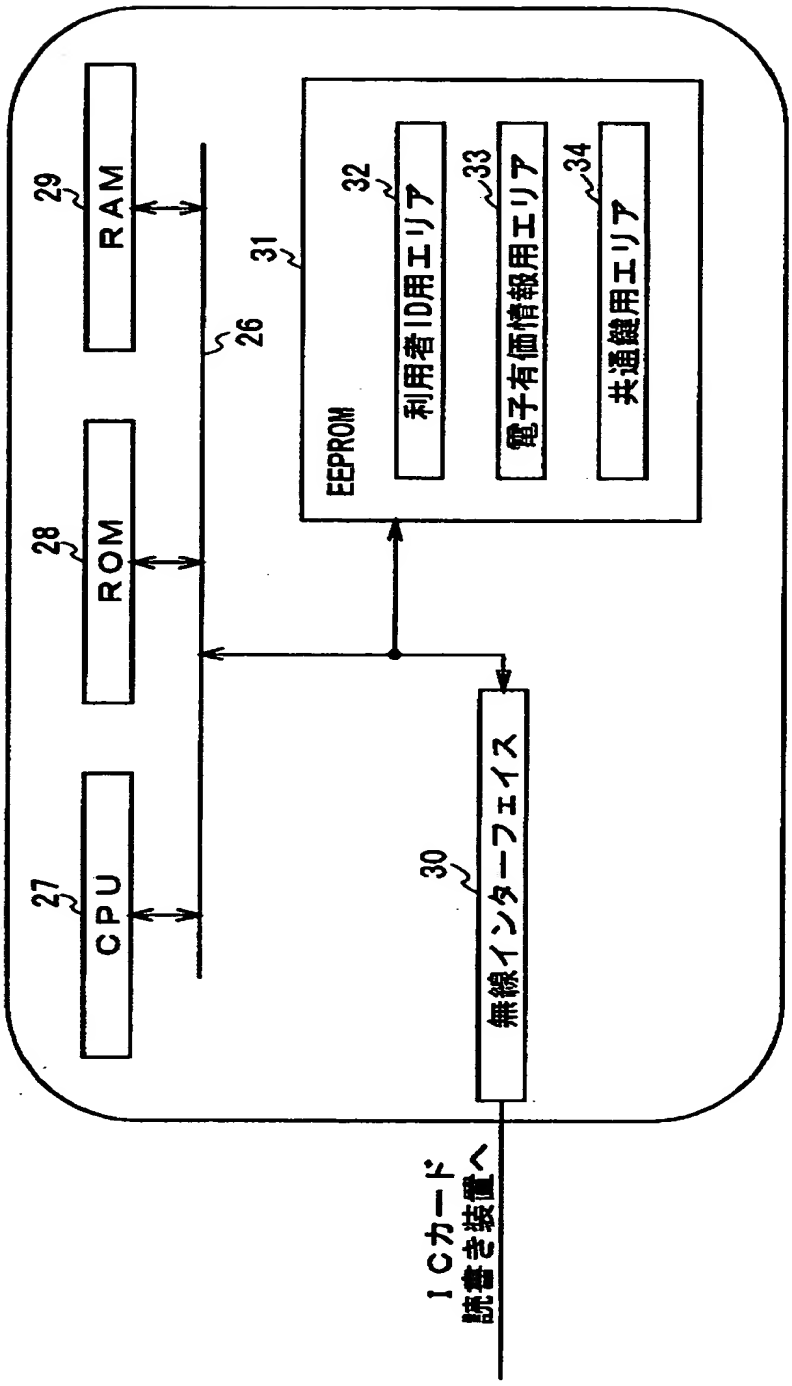

図３　ＩＣカードの構成

【図４】

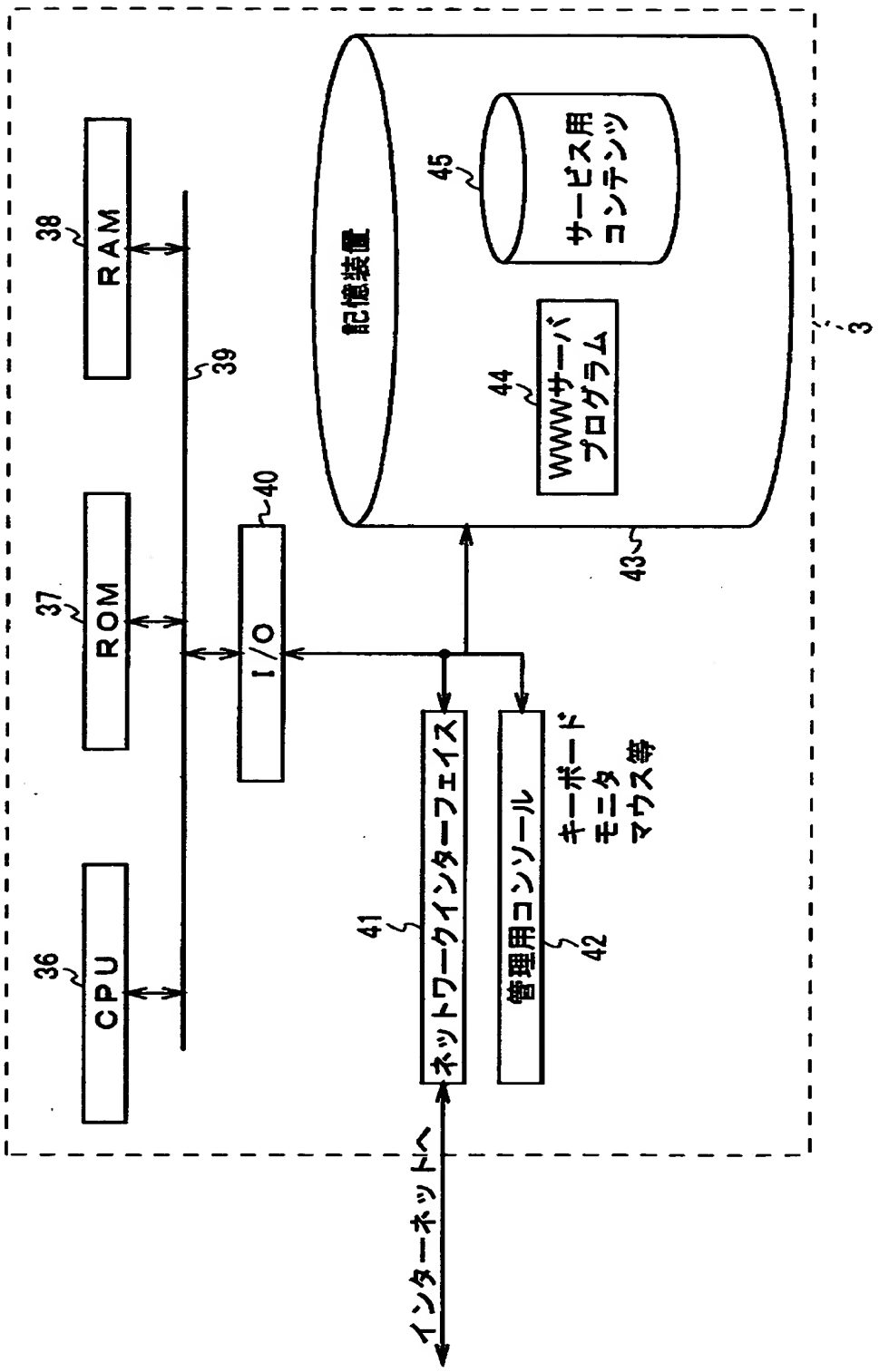

図４　WWWサーバの構成

【図５】

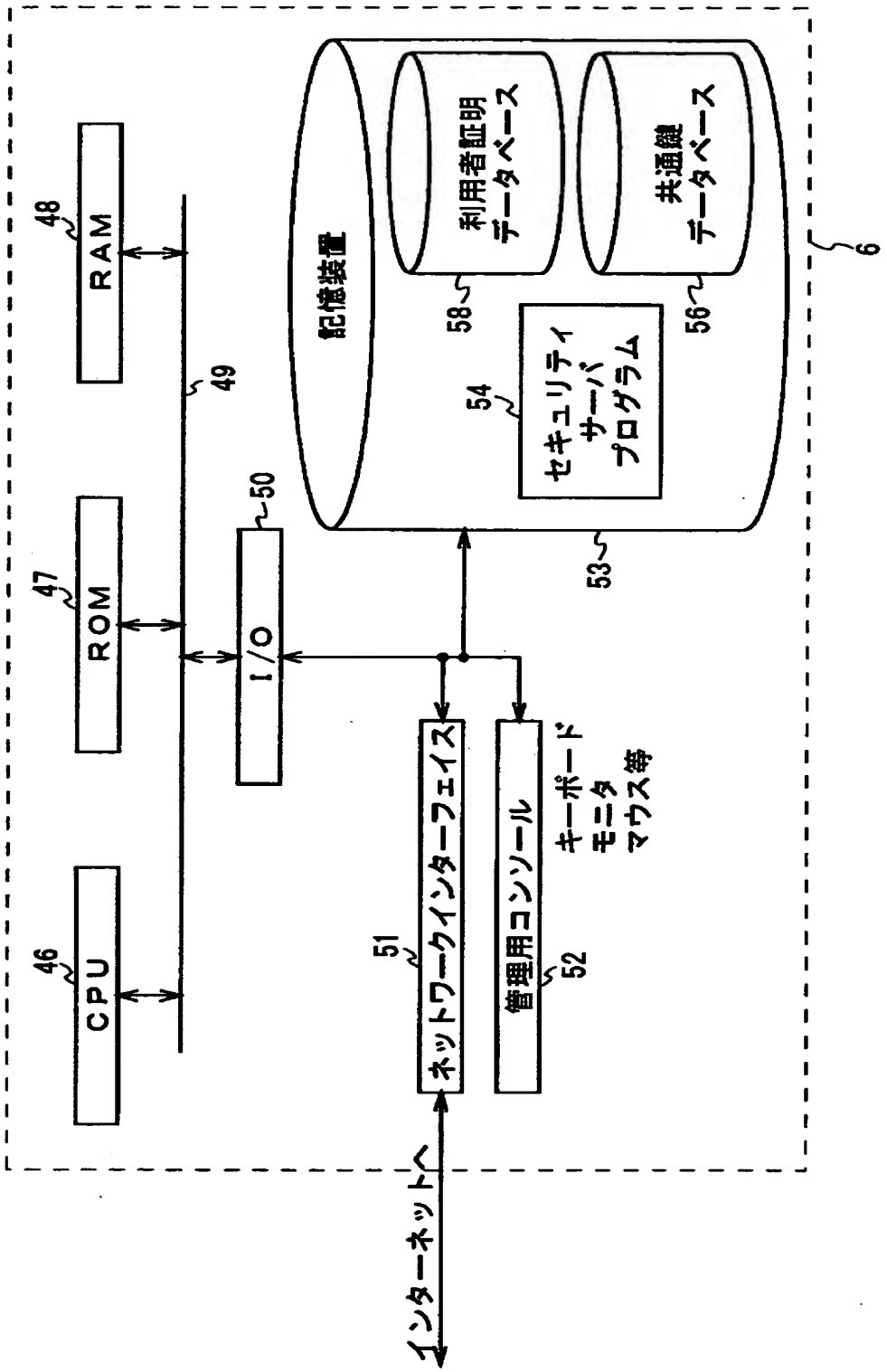

図５　セキュリティサーバの構成

【図６】

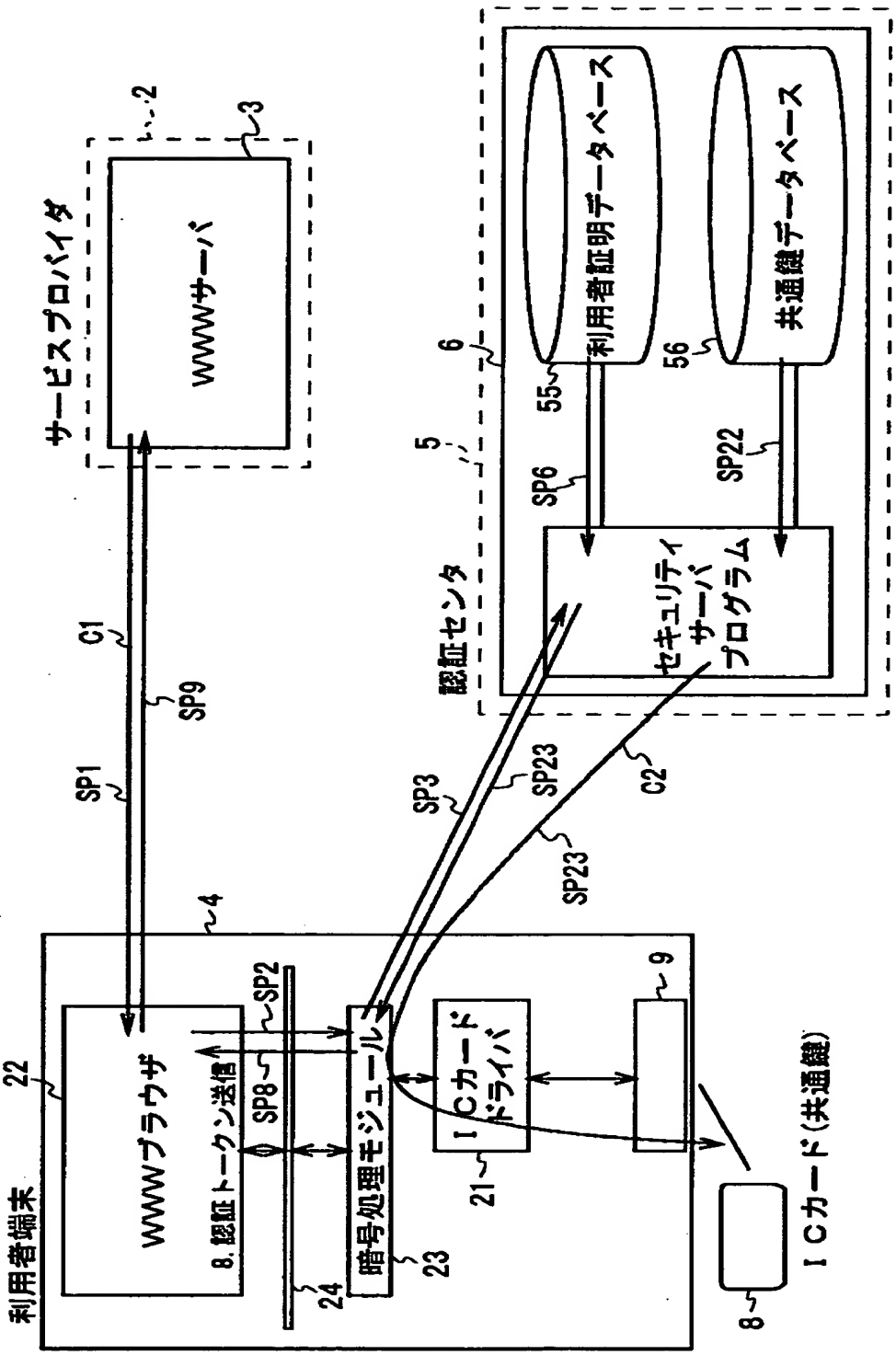
サービスプロバイダ
WWWサーバ
2
3
C1
SP9
SP1
4
利用者端末
WWWブラウザ
22
8.認証トークン送信
SP8
SP2
暗号処理モジュール
23
24
ICカードドライバ
21
9
8
ICカード(共通鍵)
認証センタ
5
6
利用者証明データベース
55
共通鍵データベース
56
SP6
SP22
セキュリティサーバプログラム
SP3
SP23
C2
SP23

図６　認証の様子

【図７】

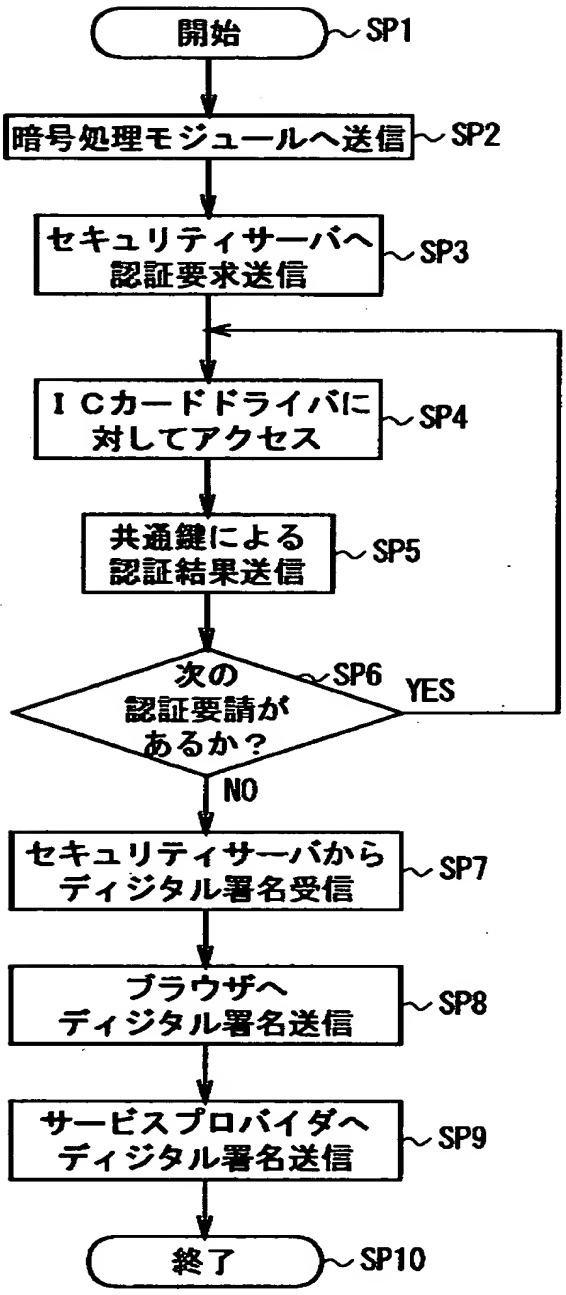

図７　利用者端末の認証処理手順

【図８】

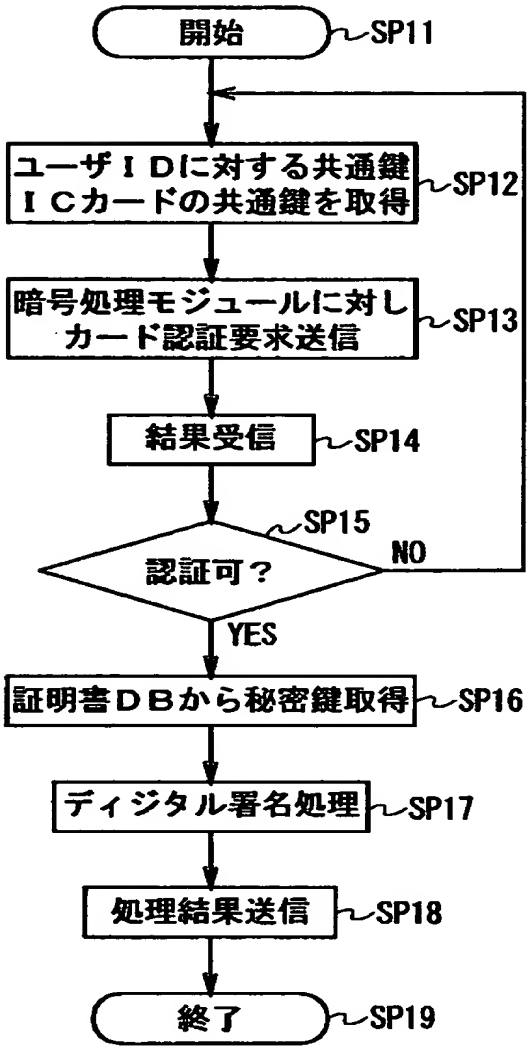

図８　セキュリティサーバの認証処理手順

【図９】

利用者ＩＤ	カード用共通鍵
0001	xxxxxxxxxxxx
0002	xxxxxxxxxxxx
0003	xxxxxxxxxxxx
⋮	⋮

56

図９　共通カギデータベース

【図１０】

57 利用者ＩＤ	58 証明書	59 秘密鍵
0001	利用者ＩＤ0001の証明書	xxxxxxxxxxx
0002	利用者ＩＤ0002の証明書	xxxxxxxxxxx
0003	利用者ＩＤ0003の証明書	xxxxxxxxxxx
⋮	⋮	⋮

55

図１０　利用者証明データベース

【図１１】

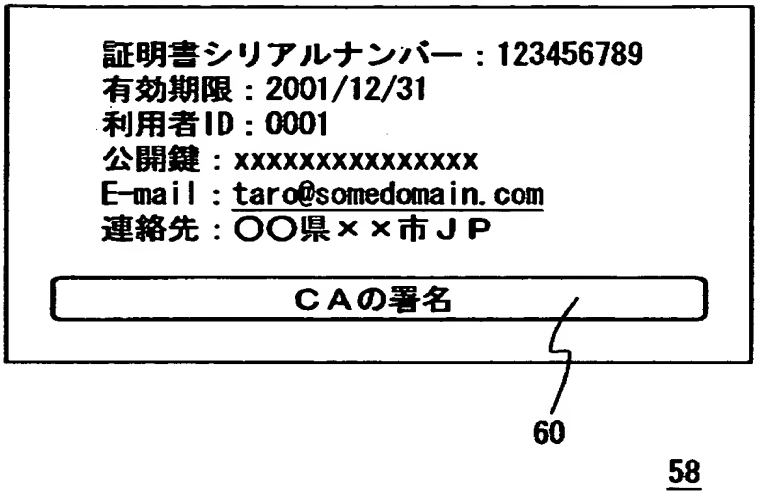
証明書シリアルナンバー：123456789
有効期限：2001/12/31
利用者ID：0001
公開鍵：xxxxxxxxxxxxxx
E-mail：taro@somedomain.com
連絡先：〇〇県××市ＪＰ
ＣＡの署名
60
58

図１１　証明書

【図１２】

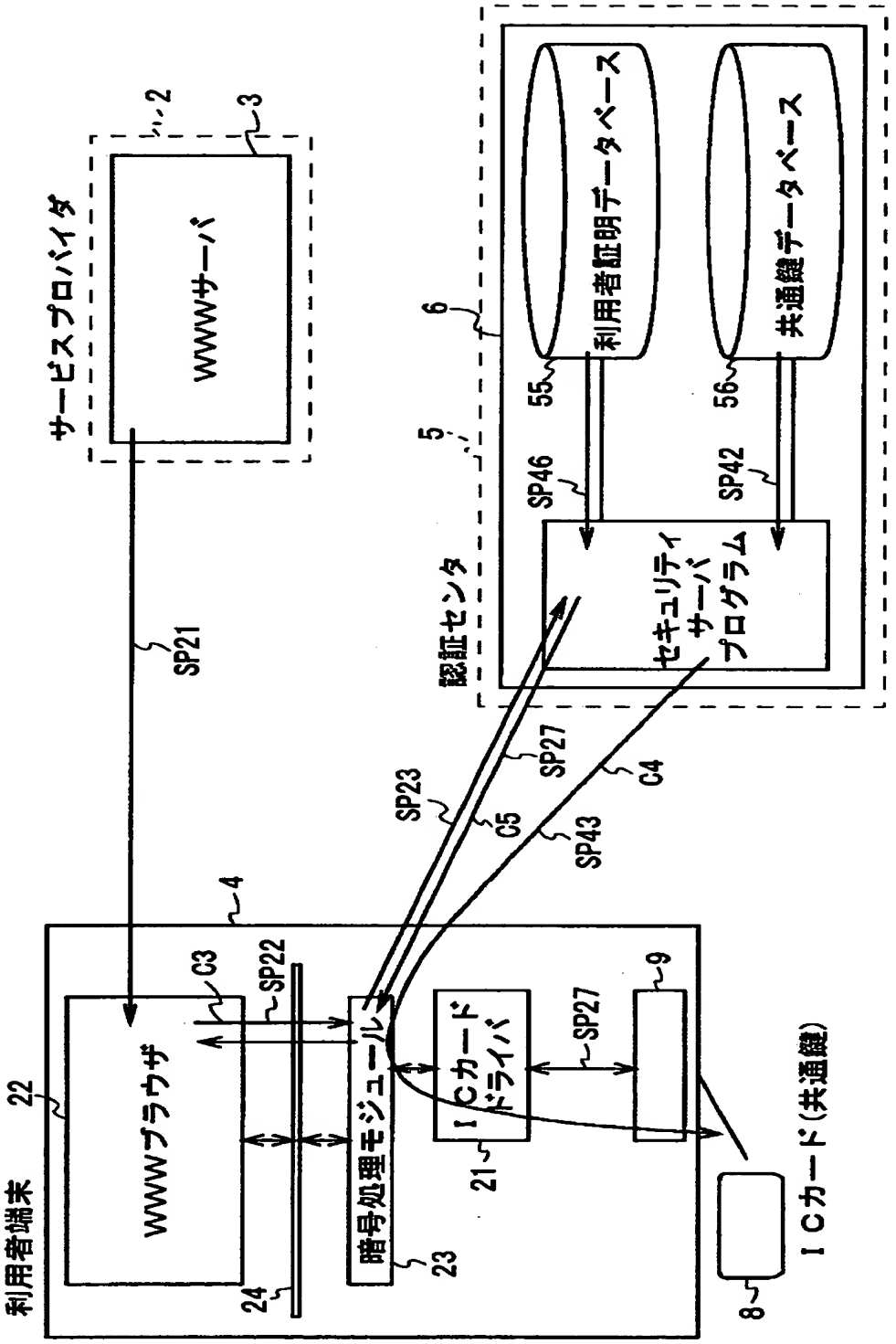

図１２　書き込みの様子

【図１３】

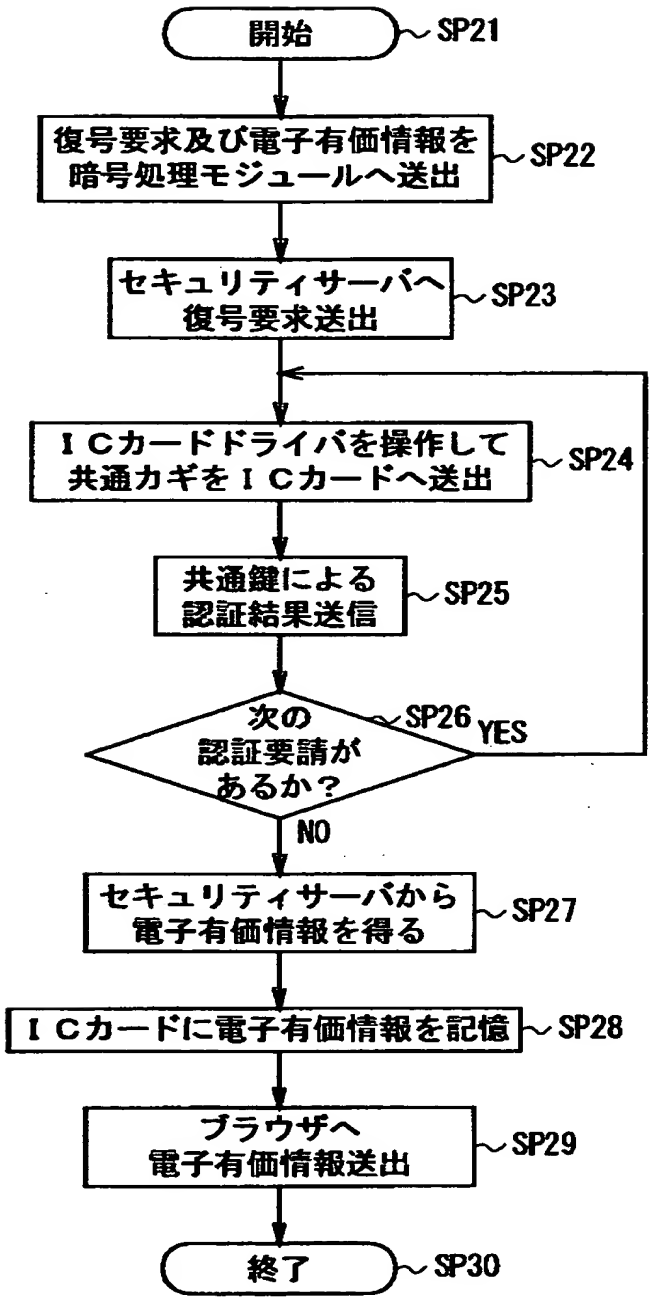

図１３　利用者端末の書き込み処理手順

【図１４】

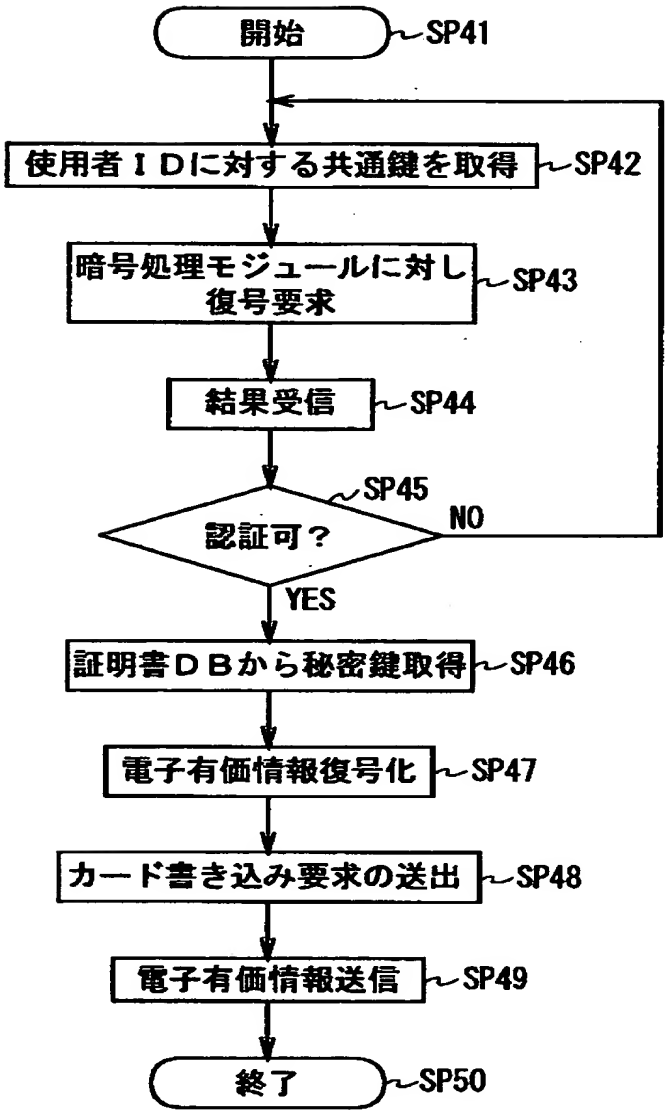

図１４　セキュリティサーバの書き込み処理手順

【書類名】　　要約書

【要約】

【課題】

公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた認証方式が望まれていた。

【解決手段】

利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させ、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにした。

【選択図】　　図６

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社